



UNITED STATES PATENT AND TRADEMARK OFFICE

A

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/061,415	02/01/2002	Davide Libenzi	002.0259.01	9282

28875 7590 07/14/2005

Zilka-Kotab, PC
P.O. BOX 721120
SAN JOSE, CA 95172-1120

EXAMINER

HENNING, MATTHEW T

ART UNIT	PAPER NUMBER
----------	--------------

2131

DATE MAILED: 07/14/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

10/061,415

Applicant(s)

LIBENZI ET AL.

Examiner

Matthew T. Henning

Art Unit

2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 01 February 2002.
- 2a) ☐ This action is FINAL. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-50 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-50 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 01 February 2002 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date <u>10/31/02, 5/30/02</u> . | 6) <input type="checkbox"/> Other: _____ |

22

Art Unit: 2131

This action is in response to the communication filed on 2/1/2002.

DETAILED ACTION

Claims 1-50 have been examined.

Title

The title of the invention is acceptable.

Priority

This application claims priority to provisional applications 60/309,835 and 60/309,858, filed on 8/3/2001.

Therefore, the effective filing date for the subject matter defined in the pending claims in this application is 8/3/2001.

Information Disclosure Statement

The information disclosure statement(s) (IDS) submitted on 10/31/2002 and 5/30/2002 are in compliance with the provisions of 37 CFR 1.97. Accordingly, the examiner is considering the information disclosure statements.

Drawings

The drawings filed on 2/1/2002 are acceptable for examination proceedings.

Specification

Applicant is reminded of the proper language and format for an abstract of the disclosure.

The abstract should be in narrative form and generally limited to a single paragraph on a separate sheet within the range of 50 to 150 words. It is important that the abstract not exceed 150 words in length since the space provided for the abstract on the computer tape used by the printer is limited. The form and legal phraseology often used in patent claims, such as "means" and "said," should be avoided. The abstract should describe the disclosure sufficiently to assist readers in deciding whether there is a need for consulting the full patent text for details.

Art Unit: 2131

The language should be clear and concise and should not repeat information given in the title. It should avoid using phrases which can be implied, such as, "The disclosure concerns," "The disclosure defined by this invention," "The disclosure describes," etc.

The abstract of the disclosure is objected to because:

Line 2 recites "is described" which can be implied and therefore must be removed.

Correction is required. See MPEP § 608.01(b).

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 12 and 27 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claims 12 and 27 recites that "the transport layer protocol" comprises at least one of "HTTP, FTP, SMTP, POP3, NNTP and Gnutella". However, these listed protocols are not "transport layer" protocols but instead they are "application layer" protocols. As such, the ordinary person skilled in the art would be unable to determine whether the processing on the datagram was based on the transport layer protocol (i.e. "TCP", "IP", etc.) or if it was based on the application layer protocol. Therefore, claims 12 and 27 are rejected for failing to particularly point out and distinctly claim the subject matter which the applicants regard as the invention.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

Art Unit: 2131

1
2 (e) the invention was described in (1) an application for patent, published under section
3 122(b), by another filed in the United States before the invention by the applicant for patent or
4 (2) a patent granted on an application for patent by another filed in the United States before the
5 invention by the applicant for patent, except that an international application filed under the
6 treaty defined in section 351(a) shall have the effects for purposes of this subsection of an
7 application filed in the United States only if the international application designated the United
8 States and was published under Article 21(2) of such treaty in the English language.
9
10

11 Claims 1-11, 13-14, 16-26, 28-29, 31-33, 35, 38, 41-42, 44, 47, and 50 are rejected under
12 35 U.S.C. 102(e) as being anticipated by Maher, III et al. (US Patent Number 6,381,242)
13 hereinafter referred to as Maher.

14 Regarding claim 1, Maher disclosed a system for providing passive screening of transient
15 messages in a distributed computing environment (See Maher Abstract), comprising: a network
16 interface passively monitoring a transient packet stream at a network boundary (See Maher
17 Column 5 lines 46-54 and Col. 7 Lines 13-15) comprising receiving incoming datagrams
18 structured in compliance with a network protocol layer (See Maher Col. 5 Lines 46-54 and Col. 3
19 Lines 54-67 wherein it was inherent that the packets were compliant with a network layer in
20 order for them to be transmitted through the network); a packet receiver reassembling one or
21 more of the incoming datagrams into a segment structured in compliance with a transport
22 protocol layer (See Maher Col. 5 Line 60 - Col. 6 Line 4); and an antivirus scanner scanning
23 contents of the reassembled segment for a presence of at least one of a computer virus and
24 malware to identify infected message contents (See Maher Col. 10 Lines 42-46).

25 Regarding claim 2, Maher disclosed an incoming queue staging each incoming datagram
26 intermediate to reassembly (See Maher Col. 8 Lines 42-51).

1 Regarding claim 3, Maher disclosed a network protocol-specific decoder decoding the
2 reassembled segment prior to scanning (See Maher Col. 5 Line 65 – Col. 6 Line 1).

3 Regarding claim 4, Maher disclosed that the antivirus scanner terminates the transient
4 packet stream if the reassembled segment is not infected with at least one of a computer virus
5 and malware (See Maher Col. 7 Lines 30-33).

6 Regarding claim 5, Maher disclosed that the antivirus scanner takes an action if the
7 reassembled segment is infected with at least one of a computer virus and malware (See Maher
8 Col. 10 Lines 42-46).

9 Regarding claim 6, Maher disclosed that the action comprises at least one of logging an
10 infection; generating a warning; spoofing a valid datagram in place of the infected datagram (See
11 Maher Col. 10 Lines 42-46); and acquiescing to the infection.

12 Regarding claim 7, Maher disclosed a protocol-specific queue staging each reassembled
13 segment with other reassembled segments sharing the same transport protocol layer (See Maher
14 Col. 7 Lines 18-30).

15 Regarding claim 8, Maher disclosed an information record storing information dependent
16 on the same transport protocol layer with the staged reassembled segment (See Maher Col. 6
17 Lines 12-22).

18 Regarding claim 9, Maher disclosed a contents record storing the contents with the staged
19 reassembled segment (See Maher Col. 6 Lines 12-19).

20 Regarding claim 10, Maher disclosed that the information comprises at least one of a
21 source address, source port number, destination address, destination port number, URL, file

Art Unit: 2131

1 name, user name, sender identification, recipient identification, and subject (See Maher Col. 6
2 Lines 20-22).

3 Regarding claim 11, Maher disclosed a protocol-specific module processing each
4 reassembled datagram based on the transport layer protocol employed by the reassembled
5 datagram (See Maher Col. 7 Lines 18-30).

6 Regarding claim 13, Maher disclosed an event correlator analyzing the transient packet
7 stream for events indicative of a network service attack (See Maher Col. 7 Lines 35-50).

8 Regarding claim 14, Maher disclosed a data repository maintaining each event (See
9 Maher Col. 7 Lines 40-48).

10 Claims 16-26 are rejected for the same reasons as claims 1-11 above.

11 Claims 28-29 are rejected for the same reasons as claims 13-14 above.

12 Claim 31 is rejected for the same reasons as claims 1-11 and 13-14 above and further
13 because Maher disclosed processors executing the described functions (See Maher Col. 11 lines
14 34-37).

15 Claim 32 is rejected for the same reasons as claims 1 and 13 above.

16 Regarding claim 33, Maher disclosed a parser parsing each reassembled datagram into
17 network protocol-specific information and packet content (See Maher Col. 5 Line 65 – Col. 6
18 Line 19).

19 Regarding claim 35, Maher disclosed a decoder decoding the packet content prior to
20 performing the operation of scanning (See Maher Col. 5 Line 65 – Col. 6 Line 1 and Col. 2 Lines
21 9-12).

4 Claims 41, 42, 44, and 47 are rejected for the same reasons as claims 32, 33, 35, and 38
5 above.

6 Claim 50 is rejected for the same reasons as claims 32-33, 35, and 38 and further
7 because Maher disclosed processors executing the described functions (See Maher Col. 11 lines
8 34-37).

9 *Claim Rejections - 35 USC § 103*

10 The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness
11 rejections set forth in this Office action:

12 *A patent may not be obtained though the invention is not identically disclosed or described as set*
13 *forth in section 102 of this title, if the differences between the subject matter sought to be*
14 *patented and the prior art are such that the subject matter as a whole would have been obvious*
15 *at the time the invention was made to a person having ordinary skill in the art to which said*
16 *subject matter pertains. Patentability shall not be negated by the manner in which the*
17 *invention was made.*
18

19 Claims 12, 27, 34, 39, 43, and 48 are rejected under 35 U.S.C. 103(a) as being
20 unpatentable over Maher.

Regarding claims 12, 27, 39, and 48 Maher disclosed separate queues for different types of transmission protocols such as E-mail, and VoIP, and web surfing (See Maher Col. 7 Lines 18-30), but failed to disclose that E-mail comprises SMTP and POP3, and that web surfing comprises HTTP. However, SMTP and POP3 were well known in the art and commonly used for E-mail and HTTP was well known in the art and commonly used for web interfacing or web

Art Unit: 2131

1 browsing. It therefore would have been obvious to the ordinary person skilled in the art at the
2 time of invention to employ SMTP and POP3 protocols for the E-mail queuing of Maher and
3 HTTP of the web surfing of Maher. This would have been obvious because the ordinary person
4 would have been motivated to use what was well known in the art.

5 Regarding claims 34 and 43, Maher disclosed extracting the header information from the
6 packets (See the rejection of claim 33 above), but failed to disclose specifically what information
7 was contained in the headers. It was well known in the art at the time of invention that the
8 headers of HTTP messages contained a source address and port number, a destination address
9 and port number, and a URL, the headers of an FTP message contained the filename and
10 username, and the headers for the SMTP contained the sender identifier, receiver identifier, and
11 subject. As such, it would have been obvious to the ordinary person skilled in the art at the time
12 of invention to employ what was well known by extracting the header information from the
13 headers of the packets. This would have been obvious because the ordinary person would have
14 been motivated to extract what was known to be contained in the header.

15 Claims 15, 30, 40, and 49 are rejected under 35 U.S.C. 103(a) as being unpatentable over
16 Maher as applied to claims 1, 16, 32, and 41 above, and further in view of Hailpern et al. (US
17 Patent Number 6,275,937) hereinafter referred to as Hailpern.

18 Maher disclosed a system for scanning IP network packets for viruses (See the rejection
19 of claim 1 above and Col. 3 Lines 54-67), but failed to disclose that all the incoming messages
20 were SMTP compliant, and therefore TCP compliant.

21 Hailpern teaches that virus scanning should be set up for each network protocol proxy,
22 including E-mail, in order to scan for viruses (See Hailpern Col. 4 Lines 1-13).

Art Unit: 2131

1 It would have been obvious to the ordinary person skilled in the art to employ the
2 teachings of Hailpern in the virus scanning system of Maher by modifying mail servers to
3 contain the scanning system of Maher. This would have been obvious because the ordinary
4 person skilled in the art would have been motivated to enable the proxies to be able to scan the
5 types of communications they already process and therefore reduce network traffic and delay.
6 Further, SMTP mail servers were well known in the art at the time of invention, and it would
7 have been obvious to utilize the scanning system of Maher in an SMTP mail server. This would
8 have been obvious because the ordinary person skilled in the art would have been motivated to
9 protect SMTP mail servers from viruses.

10 Claims 36-37 and 45-46 are rejected under 35 U.S.C. 103(a) as being unpatentable over
11 Maher as applied to claims 32 and 41 above, and further in view of Bates et al. (US Patent
12 Number 6,785,732) hereinafter referred to as Bates.

13 Maher disclosed detecting viruses in network packets (See the rejection of claim 38
14 above), but failed to disclose logging the detection or generating a warning.

15 Bates teaches that upon detecting a virus, the detection should be logged and a warning
16 should be generated (See Bates Col. 12 Lines 41-48 and Col. 10 Lines 2-8).

17 It would have been obvious to the ordinary person skilled in the art at the time of
18 invention to employ the teachings of Bates in the packet scanning system of Maher by logging
19 virus detections and generating warnings in the event of virus detection. This would have been
20 obvious because the ordinary person skilled in the art would have been motivated to enable the
21 server to analyze the virus activity and to alert the sender of the virus of the virus.

22

Conclusion

Claims 1-50 have been rejected.

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Ji et al. (US Patent Number 5,889,943) disclosed a virus detection system which reassembled packets in order to scan for viruses.

b. Tso et al. (US Patent Number 6,088,803) disclosed a system for virus scanning during download to a client.

c. Shanklin et al. (US Patent Number 6,487,666) disclosed an intrusion detection system which analyzed packets in a network in order to detect an attack.

d. Ji (US Patent Number 6,272,641) disclosed a system for scanning java applets for viruses during downloading.

e. Gryaznov et al. (US Patent Number 6,748,534) disclosed a system in which upon detection of a virus, the detection was logged and a warning was sent.


f. Rana et al. (US Patent Number 6,781,992) disclosed a queue engine for reordering and reassembling datagrams into packets in a network in order to scan them for viruses.

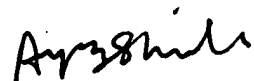
g. Magdych et al. (US Patent Number 6,513,122) disclosed a system for scanning packets for both intrusion detection and viruses.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew T. Henning whose telephone number is (571) 272-3790. The examiner can normally be reached on M-F 8-4.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).


Matthew Henning
Assistant Examiner
Art Unit 2131
7/6/2005


AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100